A Proactive Framework for Detecting and Preventing Cyber Threats on E-Learning Platforms

SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna International Institute of Research and Studies

(Deemed to be University)

by

Bhoopendra Singh

Registration number: **19/Ph.D/091**

Under the supervision of

Prof. (Dr.) Brijesh Kumar

FACULTY OF ENGINEERING AND TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD – 121001

FACULTY OF ENGINEERING AND TECHNOLOGY

Certificate

I hereby declare that the short synopsis "**A Proactive Framework for Detecting and Preventing Cyber Threats on E-Learning Platforms"** being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in **Computer Science and Engineering** under faculty of **Engineering and Technology** of Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2020-21

It is a bona fide record of original work carried out under the supervision of **Prof.(Dr.) Brijesh Kumar** and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is plagiarism free and proof has been submitted.

(Bhoopendra Singh)
19/Ph.D/091

(Prof. (Dr.) Brijesh Kumar)
Signature of the Supervisor
Faculty of Engineering, MRIIRS Faridabad

(Chairperson, DRC)

ABSTRACT

Abstract—As the use of internet led to exponential and enormous changes in the life of an individual in the context of various emerging factors like social and economic welfare, cyber fraud, cyber espionage, cyber crimes and others various unethical and unlawful activities .The effects of these evil practices are not only affecting to the various Government / Non Government organizations, but also leaving a major concern to e-learning portals of higher educational / research institutions, academicians, researcher, practitioners and students of various academic institution. The major impact factors of this are like dealing with privacy, protecting confidentiality, and safety of all users for safeguarding against the various cyber attacks executed by hackers and cyber criminals. The most important asset of any HEI's are their research works, digital repositories and various other e- resources offering its uses to its students and other stake holders. It is the prime responsibility of these HEI,s to provide the adequate security and safety of these portals and devices like servers, storage, firewall, switches, routers and others network and communication devices. E-learning portals are effectively optimizes the existing information technology and networks resources of the internet. They are also equipped with various stakeholders, effectively distributed digital resources in the form of various databases in order to protect the existing requirements for confidentiality, authentication, and privacy. This research work focus and highlights the various flaws of cyber security and will proposes a suitable security model which will protect the E-learning portals of HEI,s against various cyber attacks. Since this is a most concern area in today's era of internet to analysis cyber threats, considered to be the Major setback for E-learning platforms. The proposed security model and its infrastructure, facilitates the Information Technology Administrator to ensure the resources which are to be shared through the e-learning portals of higher education institutes needs to be secure from any kind of cyber attack.

Keywords—Cyber attacks; unlawful activities; E-learning; Major Failure; Security model; security threats

CONTENTS

S. No.	Description	Page No.
1	Introduction Abstract 1.1 Introduction 1.2 Cyber Security and Higher Education Institutions (HEI,s) 1.3 Digital Resources in Higher Education Institutes (HEI,s) 1.4 Government Initiatives towards enhancement of IT Infrastructure 1.5 Cyber Security Concern in the Present Security Models of E-Learning of Higher Educational Institutes 1.6 Cyber Crimes 1.7 Cyber Security 1.8 IT Infrastructure of Higher Education Institutes 1.9 IT Security Measures by Higher Education Institutes 1.10 Disaster Management by Higher Education Institutes 1.11 Cyber Security Awareness	5-17
2	Literature Review	18-27
3	Problem Statement	28
4	Research Objectives	29
5	Research Methodology 5.1 Selection of Sample 5.2 Sample Size 5.3 Sources of Data 5.4 Data Collection Method 5.5 Data Analysis	32-34
6	Expected Outcome of the Research	35
7	References	36-38

1.1 Introduction

Information and Communication Technology has shown a vital impact and positive effect on the process, progress and development of peoples and its related society. The rapid growth and enhancement in the use of Science and Technology have come up with unrealistic progressive changes and vital improvement in the process which is being followed by present higher educational Universities and Institutes. Due to the inception of this information and communication technology, flow and exchange of information through online or web mode have consistently accelerated in the present education system as well as in the present civilized society. Universities and higher educational institutes often meeting with the challenges coming out of the use of its critical resources in the form of huge digital repositories storage and management. The kind of information it process and its retrieval, and exchange these digital repositories in various forms among the other universities and its stakeholders. Faster growth and massive advancement of its digital repository in the recent few years have brought contemporary improvement in the concept, planning, execution and control of organization in smooth functioning of higher educational institutes.

Adoption of latest and automation enabled technology has highly enhanced the scope of e-learning mode of education by extending the various digital in house and subscribed repositories to its stakeholders. In true sense, it can be undoubtedly said that the capabilities of providing the safe online digital education has immensely managed the flow of the information in a safe and secured manner. The use of Information and communication technologies has brought the unpredictable enhancement with ease of access for its users and stakeholders. Due to the inception of atomized use of application, the area of education in e-learning portals has touch the remarkable boundaries for extending the various digitized resources for the users around the world having no geographical boundaries. Cyber attacks on these higher education e-learning portals in the various forms not only affects the technical services of HEI's, shapes the Information technology services that are being distributed among public. HEI's use various IT enabled automation tools to carry out the overall management of digital repositories and its uses along with managing and controlling of various other academic, administrative, accounts and library services of higher educational institute. University Automation is one of the major applications of IT in helps to change the institute in-House activities (Academic, Library,

Account, Procurement, examination, admission and student life cycle kinds of things etc.). In this context, the use of Cyber and Information Communication Technology contribute the major role of security for protection of in house and subscribed resources of higher educational Institutes. Based on this concept the research focus is to analyze the drawbacks of cyber security mechanism practices adoption in higher educational Institute and its security with inception of a proper cyber security model will cater the need and challenges faced by the universities and its stakeholders"(M, 2014). Higher Education Institutes (HEI,s) in India are considered as Most emerging Institutions in imparting the Education and Research activities. IT Infrastructure and IT Security of these Universities are most critical area which provides complete exposure to its in house and subscribed academic/ research repository or can say the digital collections of various databases. IT Infrastructure is one of the most sensitive area which facilitates, to a clientele for helping the operational objective and to achieve its mission and goal of the parent organization (Seidman, 1991). The IT Infrastructure is the backbone in the imparting services to various stakeholders of society (Frederic, 1964).

1.2 Cyber Security and Higher Education Institutions

The primary concern of (HEI,s) in Information technology is highly revolutionised. On one hand the Information technology reduced the task of university in retrieving and disseminating the information. On other hand, the institutional Resources' has shifted from locally storing information to facilitate the users by creating, disseminating and sharing the information worldwide. The Academic need and requirement have changed their traditional approach, Higher Education Institutes are using Cyber and information security not only to provide the on campus facility, access of subscribed resources but also developing digital resources, tools and techniques and infrastructure to serve the researcher without any space barriers. There is a rapid demand in accessing the information available in a multiple formats without any space barriers, considering the same the tools are regularly incorporated in the IT system. Modern and innovative technology enables academicians to promptly understand the highly growing horizon of innovative technology. It may facilitate a different kind of pattern of examination in the form of test to Institute (Wertkin, 2014).

In this era of Internet, online portals and education systems are more expanded and became the essential need of our modern culture and society. Since the online portals and e-resources are to be distributed and shared to all authenticated stakeholders and the internet is the backbone to

grant the access to these portals due to which these systems may be the victims of various cyber threats like software attacks (denial of service, macros, viruses and worms), espionage, acts of theft (illegal mode of stealing data) and intellectual property (piracy, copyright, infringement) etc. In order to mitigate the cyber challenges and security risks of these portals, the organizations need to frame the proper security and disaster management mechanism in the forms of secure policies and workable models. Security of e-systems are the prime need and essential activities so induction of new tools , technology, system and network security, development of secure applications should be the top most priority of organizations to be adopted and followed. Any kind of security hazard should be properly assessed and the corrective measures in the form of solutions are to be incorporated to avoid such security flaws in future. For better understanding and to provide the suitable solutions, the required quantitative or qualitative research has been carried out to enhance the policies guidelines, good plans and developing of security models.

Cyber Security is emerging as a wider and essential need to analysis the security impacts in order to carry out the various organizational and professional activities in the Higher Educational Institutions .It also acts as an key instrument to cater the academic and professional need of all its citizen and stake holders on various domains like Medical, Engineering, Social Science, mass communications and Legal platforms etc in a secured manner.

- **E-learning portals** are playing the major role of being the interface between the education providers and education seekers (Rahim, Othman, & Hamid, 2020) .It is one of the best way of learning by using the internet sources and electronic devices like laptops, Desktops, Mobile phones and other electronic gazettes. These systems are so fine that the delivery of education can be done by using the various important resources in the form of digital contents and does not requires the physical presence of stake holders in any way. E-leaning being the latest and most demandable concept of learning which provides the opportunity to all needy people without fixing any geographical, regional, time and space constraints.

- **Learning Management System:-** It is software application which manages the education administration, admission process, student resources, assignments, digital resources, reports, training programmes and delivery of educational courses with the kelp of internet and without being compulsion of physical presence of students.

Information and Communication Technology being the resources carrier collaborates and provides efficient communication to all the concern and help them in providing the required access of all existing digital resources and materials of e-learning portals.

1.3 Digital Resources in Higher Education Institutes:- Higher Education Institutes are very unique in terms of their role and imparting the education and building the societies; the Universities are enriched with very special IT Infrastructure and its associated devices. The IT Infrastructure consists of Middleware, Monitoring and Tools, Network, Network Security, Server Infrastructure, Storage, and Databases. Digital repositories consist of research works, e-books, Monographs, Treatises, Government Publications, Constitution of all nations, Parliamentary Debates (Lok Sabha & Rajya Sabha), Gazette of India, Periodicals, Reports, CD-ROMs and digital databases. This information's are also using special techniques to store and access the collection. With the advancement of technology the Higher Education Institutes (HEI,s) are not only subscribing various databases but also finding the resources available free of cost through internet, creating their own Institutional repositories, and participating and coordinating with various government initiatives. This will help the libraries to provide the access of maximum resources & to cater various information needs in limited budget.

1.4 Government Initiatives Requisite IT Infrastructure

Digital transformation of information's is bringing drastic development in extending the multiple variants and mode of delivering the education and also exploring the possibilities in staggering the future goals of stakeholders by adopting these e-learning model in the Higher Educational arena. During this ongoing pandemic (Covid-19), these e-learning portals emerged as a life saviour in terms of imparting the education as well as sustaining the professional growth. Most of the Universities /educational institutes come up with various initiatives and start-ups by the support of Government of other agencies to aiming the object of educational needs to promote digital learning. The technological Innovations and digital initiatives has all the possibilities to revolutionize the higher education system in India. Majorily, all the Academic and Research organization of the country have adopted digitized way and designed its all the existing resources in digitized form / repository for the benefit of the Researcher, Academicians, students and other professional entities. Some of the Indian initiatives

are mentioned below.The success of all the following initiatives depends on the smooth and uninterrupted IT infrastructure.

- **Swayam: "Project Swayam has been designed by the Ministry of Education,** Government of India to offer various courses in online mode. It has been established as strong e-learning platform to disseminate the education to each needy person from far flung and remote area using various digital resources and digital repositories."
- **MOOCS:"**Massive Open Online Courses (*MOOCs*) courses have been designed by the various educational experts in the forms of modules to enhance their academic and professional skills and playing instrumental role in career development and providing the quality education to citizen. "*MOOC*.org is an extension of edX.org, a leader in online courses".
- **National Digital Library of India:** "It is platform in the form of **S**ingle Window system that provides a platform to collect the metadata from most of the renowned organization in country imparting the education with in India or abroad. Most of these institutions generate a digital repository by sharing the meta data of their resources through API for easy implementation through software.
- **E-PG- Pathshala:** This covers most of the subjects /domains of education system and provides quality material of all the area in the forms of vedio lectures, digitized material. The Link to access the collection is http://epgp.inflibnet.ac.in/ .
- **Shodhganga:** This is the repository of Indian thesis and dissertations submitted to universities.
- The Link to access the collection is http://shodhganga.inflibnet.ac.in/
- **Shodhgangotri** : This repository is maint for keeping the synopses and proposal of research for PhD programmes conducted by the Indian universities.

1.5 Cyber Security Concern in the Present Security Models of E-Learning of Higher Educational Institutes

As we know that there are various cyber security concern in the present security models of e-learning of higher educational institutes. Few of them concern are given below to understand and analyze the security issues for proper rectification in the form of secure e learning module

1.6 Cyber Crime

Cybercrime can be defined as the criminal activities that are carried out by means of the Internet or a computer. One can consider cybercrimes as the use of Information technology for criminal activities. In Cybercrime, a computer might be used in the commission of a particular offence or crime or it may even be the target. With the development of cyberspace and internet criminal activities over internet have rapidly expanded and evolved in unexpected ways. The speed, convenience and anonymity offered by cyberspace is exploited by criminals today for committing a wide range of cybercrimes. The voluminous expansive use of the internet leading to large online population has therefore, made many people vulnerable to Cybercrimes. Several countries across the globe are reporting towering losses due to the cyber-crime worth billions of dollars. Cases of Cybercrime are continuously rising, many cases of cybercrimes like, data fraud, hacking of personal accounts and many others have been reported. Private entities, critical information infrastructure (CII) and many others face severe risks from cybercrimes (Parodi, 2013). Cybercriminals are embracing innovative techniques for executing diverse criminal activities in cyberspace. Although, governments across the globe have taken enormous measures to address the issues and challenges of cyber-crime like, Indian Parliament amended the IT Act, 2000 providing legislative provisions for cybercrime, the constitution of The Indian Computer Emergency Response Team that issues alert as well as advisories with regard to the latest cyber threats, countermeasures, etc. However, more steps must be taken considering the complex and dynamic nature of cybercrimes which are not limited to a particular country's geographical boundary.

1.7 Cyber Security

The expansion of internet is very vast having undefined boundaries similar to the use of any highway without any safety rules or regulations. Its use is very close to a person riding on a bike and speeding the same without any safety device like, helmet etc. The same algorithm is applied to all the users of internet. There are billions of users existing on web without knowing any identity, role and nature of user. Anyone of them may be a

person having malicious intention and may cause huge loss in the forms of various cyber frauds. In the journey of internet, one can be a victim of many malicious activities and can face the huge loss of assets and information's. Presently, the required regulation or proper guidelines are not there to control such fraud activities. It is an open space which can be access by anyone for their respective uses the way they want. The wide scope of operations and utility of cyberspace today has enabled the cyber world an undeniable level of impact in almost all sectors of economy and other operations of society which can't be disdained by any entity. The Internet has become the backbone of everything in society today, from delivery of food to waste and traffic management its use is incredible. Moreover, Internet due to its usage has befitted itself to be called as the backbone of backbones since; critical infrastructure (like-banking, power supply, railways, nuclear power stations), national defense, as well as the daily lives of people rely significantly upon computer-driven & interconnected information technologies. The Internet can therefore, also be attributed as the basic infrastructure of everything. Further, it can also be regarded as the lifeblood of all networks since there has been ratification of almost everything. Data today is considered as the new oil which is driving today's modern economy. Everything today is being metamorphosed and incredibly reduced to data. Moreover, in today's modern age smart phones have become an intrinsic component of a person's life. There has been a seamless merger of an individual's online as well as his offline life which shows that the dependence of people over the Internet is increasing continuously (Koops, 2016)

1.8 IT Infrastructure of Higher Education Institutes

(i) **LAN**: - It's a kind of IT infrastructure which required to setup locally for accessing the internet and its all existing resources. LAN can be setup as per the need of the higher education Institute by extending and restricting the digital and other resources. It can also be used to sharing the digital repositories and other existing hardwares in the forms of computers, printers and other hardware devices like network switches, network attached stores and media.

(ii) **WAN: -** WAN stands for Wide Area Network required to setup in any higher educational Institute for accessing the internet and any other information

available on World Wide Web. It is also required to connect multiple LANs available in different-2 Campuses of a academic institution.

(iii) **INTRANET: -** Intranet is used in a small setup kind of academic environment. The functionalities and its operation remains same as the Local Area network (LAN).It means that the tasks which can be undertaken by LAN environment can also be taken over by the Intranet.

(iv) **WIRELESS NETWORK: -** Wireless setup is also known as Wi-Fi setup which is a major network provider medium of any academic Institute. It consists of a Wi-Fi controller and connected with few Access Points (APs). The major concern of this network is to maintain its security for extending and restricting the access of internet and its resources**.**

(v) **PROXY SERVER:-**Proxy Server is used to access the Institutional repositories from off- campus location. It's a safe and secured way of accessing of subscribed databases and all existing digital repositories by any of the user having the access through Proxy Server.

(vi) **VPN NETWORK**:- VPN is also known as the "Virtual Private Network" used to gain the access of internet or the repositories in same environment which exist in the campus.VPN access provides an authenticate user a similar configuration of setup as he or she feels while being in the campus.

1.9 IT Security Measures by Higher Education Institutes

(i) **Local Authentication:-**It's a first step security measure undertaken by the user for gaining and restricting the access to the computer. Its should be as per the need of existing IT security policies of the Institute and meeting the criteria of domain. A proper guideline to be followed while changing the password and a proper care must be taken to avoid sharing the password with others.

(ii) **Firewall / UTM Security:-** Firewall is protection mechanism available in the form of an hardware and software and used to protect and prevent the internal network with external network. The Firewall can be configured with various security policies for granting the access to the users and security devices with defined role and responsibility. It can be configured to prevent the different kinds of cyber attacks from external world and different kinds of virus attacks.

This device can be configured with various access of other LAN network with defined policies and guidelines.

(iii) **Centrally Managed Antivirus Server: -** Centrally Managed Antivirus server is used to prevent the Computers and Servers from various other virus attacks, spyware attacks, Trozen horse. Ransom ware, anti spyware, log manager and other various attacks etc. The major concern of this antivirus is update its definition regularly every after fix interval of time.

(iv) **DMZ Zone for Server Segregation:-** It's a special and separate zone defined in any Unified Threat Management devices or Firewall for the operation of its Servers kept in high security zone of configuration.DMZ is also known as De-Materialized Zone which is different from normal network zone and maintaining the very high security and prevent the accessing of existing servers from any kind of unauthorized access and cyber attacks.

(v) **Intrusion Prevention and Detection System:-**Intrusion Prevention and Detection System is a part of any hardware or software to detect any foreign attacks which can be in the form of an intrusion. Any threat if, detected then it is also used to prevent from these kinds of foreign attacks.

1.10 Disaster Management by Higher Education Institutes

(i) **Regular Backups and Data Recovery:-**Disaster Management is a most important area of any academic university which comes into the operation in case of any disaster. This is a area where the backups of all critical servers and computers are kept in a secured manner with a regular interval of time. In case of any disaster, these back ups are needed to restore the configuration of any critical devices and resource existing in the servers and computers.

(ii) **Standby Critical Servers:-** This is a area where the stand by servers and computers are kept on the network with same and live server configuration and it can be used in case of scaling down of any servers and machine with no or less downtime. These servers and computers are kept in clone mode of configuration which updates in the concept of heartbeat concept. The same thing is also applicable to all existing hosted applications on the servers and other hardware machines.

1.11 Cyber Security Awareness

Awareness is the initial step to be taken to reduce the number of cyber attacks and frauds in the form of any kind of thefts affecting the digitized resources or may be in the form of personal information attacks. It is one of the formal ways to avoid and prevent the cyber crimes. There are many ways to aware the citizens to update the various kinds of frauds and threats happening in the present time. Most of the people are not aware about all the ongoing threats and crimes so it is the responsibility of all professional and expert to carry out the awareness campaign by organizing the workshops, conferences or the lectures with live and practical instances. In order to implement the security, the first step is to have a strong login password which can have the combination of letters, symbol and special characters with fair length of characters. Keeping the strong password prohibits and deny the unauthorized access to the machine and act as a strong gateway. It is recommended that the assigned passwords are to be encrypted with suitable encrypted algorithm to safeguard against the various attacks by the hackers and fraudsters. There are enormous way to crack and bypass these password by adopting the different techniques and led to compromise the entire system. Encrypting the passwords and other valuable information enhance the security. Every second there are finite changes and value addition in technology, which operates in both ways of securing and making vulnerable". There is a misconception among the people who think that installation of antivirus or spying software's in computer is the protection from threats. Likewise, it is believed that doing so, will save the individual from various internal and external attacks which is not true. The proper awareness among the people and societies need to spread about ongoing cyber threats and challenges and risks associated with it. It is also required for them to keep their devices with authenticated software's and should be up to date. In order to avoid or counter these attacks users need to understand the pro and cons of these attacks like phishing attacks in terms of misspelled words, fake names and fake web links. Many people have been victimized for phising attacks.

(i) Phishing Exercises through Stimulation

It is one of the main factors in the form of stimulating phishing which can be used aware and train all concerned in the form of researcher, academicians, administrators and students. It can be easily promoted and understood by setting up various campaigns and programmes related to the different kinds of phishing attacks for targeting the higher educational institutions. Various practical exercises in the form of demonstration may be conducted by the IT and Cyber team to avoid these phishing attacks. The emails, Whatsapp or normal message received from any platform or social media are to examine carefully before carry out and further process of execution. The phishing attacks may be in the form of any attachment of .exe file or it may also be in the form of any web link. Whenever any user tries to execute any of the suspicious links may lead to any fraudulent and may be a victim of the attack resulting the loss of personal information or any financial transactions. This kind of awareness may be extended in the forms of video, games or any kind of modules in order to have the better understanding and knowledge. The higher educational Institutes need to take proper concern to avoid any kind of phishing attacks.

(ii) Sharing of Digital Resources

All the relevant stakeholders consist of researcher, students, administrators and academicians are required to access the institutional digital repositories through various modes of sharing. Most of these resources are being shared through remote access facility by using their Desktops, laptops and smart phone devices. These resources can also be shared be using the various modules of E-learning like NPTEL, Swayam and MOOCs platform. Any of the person having malicious intention or may be the hacker may always try to hack these resources. So it is the prime concern of IT administrators of Higher Education Institutions to prevent these digitised resources from any kind of foreign attack or any other cyber attacks. The IT administrator needs to implement the proper IT security guidelines and Policies to counter these kind attacks. They also carry out few dummy exercises for users to take the preventive measures in

case of any mis happening or to act in case of occurrence of such activities.Although there are various application or app being used by the stakeholders to carry out these activities to have access of these institutional repositories in the form of digital resources. So it is required that everyone should be aware to choose the desired app in a very protected and safe manner. The access should be extended as per heir role based for its stakeholders to have a proper monitoring and controlling of the resources. In case any hackers happen to gain access to any of the professional or personal data, it may lead to gain the access to your personal account of emails, Institutional account and bank accounts. Therefore, the sharing of resources should be carryout in a very protected and safe manner and it should be protected by various intrusion prevention systems, intrusion detection systems and by using software and hardware firewalls.

(iii) Incentives for Informer or Achiever

Incentives can be awarded to those people who take more interest in understanding and bringing any harmful information about any of the malicious activities. If anyone of them comes up with any major security attacks or may be threats, his morale must be boost up by encouraging his contribution and he may also awarded some incentives in the various forms these kinds of incentives not only boost up the confidence of individuals but also deepened the interest in achieving the education.

This initiative enhances the interest of users to be as a keen observer of various types of cyber attacks and its preventive measures. With this offer an user always tends to curious about the fault finding cause and its remedy. In this way, the higher educational institutes may encourage its scholar, staff and academicians to offer a valuable prize in the form of an award. The important outcome of this technique is to engage in these activities is to find out the attack and can engage the required defensive techniques to overcome all these issues of cyber attacks.

(iv) Institutional Awareness on Security Hygiene

Security guidelines and policies play the important role for maintaining the security challenges to counter the cyber security challenges in higher educational institutes. In order to provide access at different levels to different stakeholders, it is required to all of them to grant the dedicated access of concerned databases. The security policies are deployed to prevent the attacks from outside world. By deploying the various IPS/IDS policies and dedicated firewall in the form of hardware and software's.

2. Literature Review -(Ulven and Wangen, 2021) The computer security requirements in HEI's being exponentially increasing. Seriously, data violations occur and can occur again without adequate risk management. This article is a comprehensive reference to combine research at risk of cyber security by examining the existing literature of known assets, threats, threats and vulnerabilities (CLR applies models. This review contains studies issued from the last 12 years , with the aim of expanding the understanding of the important areas of risk of cyber security. The main discovery was , but there is a great gap in because an empirical research on the risk of cyber security in higher education is scarce. Despite this problem, our analysis has found a high contract on the issue of cybersecurity between the revised sources of information. In this document, we combine the summary of the critical assets of the mission, propose daily events of threats, we propose a general threat model and summarize the common vulnerabilities of cybersecurity. The explained report defines the outcome as nine strategic risks with a frequency description of the executed data set and the results. These outcome provides as entry for the safety of professionals in HEI's , in terms of taking care in research and developments for forthcoming work. It is serving as a start point related to the security of researchers.

(Alexei and Alexei, 2021) The Covid19 pandemic essentially affects the learning association of advanced education foundations (HEI). Since March 2020, distance instruction is the solitary opportunities for the proceeding with training measure. Distributed computing, internet learning stages and video conferencing applications, under the states of the Covid19 pandemic, the generally restricted utilization of in advanced education organizations has become the primary resources for web based learning. Therefore, experience the ill effects of DoS/DDoS assaults, cross-site prearranging, ridiculing, unapproved information access and the danger of disease with noxious projects, and the danger of individual information being taken has expanded drastically. The exploration depends on distinguishing sorts of assaults that fundamentally affect resources, yet additionally proposes to further develop network security in e-learning conditions. Normal ideas incorporate refreshing the framework and overseeing security patches, executing access arrangements at the application or asset level, grouping data, and utilizing encryption conventions.

(Cojocariu, Verzea, and Chaib, 2020) The experience of ongoing years has uncovered an issue that can influence our day by day lives: cybercrime. In advanced education

establishments, this issue is intense on the grounds that the number and kinds of gadgets that can be associated with the information network have expanded by . This issue is likewise influenced by the idea of instruction and examination exercises, which include an enormous number of showing staff, assistant or non-showing staff and understudies, just as perplexing PCs and exploration frameworks in different fields. Individuals from advanced education organizations might become survivors of different digital assaults (social designing, DDOS assaults, Trojan ponies, infections, and worms), or need to discover variations of winwin as effectively as could be expected. You can change some of them over to Internet Crime. Discovering limited admittance variations of with various security boundaries is basic to the appropriate activity of the schooling and examination measure in these kinds of establishments. In this unique situation, the objective of examination is to distinguish and order the principle dangers and assaults on the information organization, just as the different data and exploration at present looked by advanced education establishments. These issues ought to be managed most genuinely, on the grounds that by and large, the end of digital assaults is completed after the digital assault is done , so all or a piece of certain information will be lost, and the production of a security obstruction might confine admittance to assaults The individual kept private. Institutional data. The outcomes assisted with opening up another examination course , prompting the improvement of a security the executives model reasonable for scholarly exercises.

(Maranga and Nelson, 2019) Higher educational institutes and the respective e-learning portals involves various kinds of digital transactions in the form of sharing institutional repositories. This process is being achieved by using the expensive third party tools in the different role of various applications and exposed to serious attacks and threats. Protection of these existing resources from outer world and other security related threats are the responsibility of these higher educational institutions The cyber attacker and fraudulent are constantly making their efforts and try to find out the easiest way to break the existing security and mislead the information. The review of this paper states that the higher educational institutes are highly prone and attackers are making them their easy targets, so in order to prevent these attacks dedicated and secure models of network security is essential to overcome these ongoing issues. Sequential and updated Literature Review needs to be followed to understand this issue from the core. Higher educational institute has to monitor

these activities in a much secured way as there are chances that anyone out of existing stakeholder may be the victim of carrying out such activities.

(Potgieter, 2019) Most of the times the Cyber security awareness (CSA) is neglected by most of the users of higher education institutes. Due to the emergence of various threats and ongoing cyber attacks the awareness of covering these serious issues are utmost required. Therefore, a systematic process is to be designed and implement for all its users to understand the nature of threats and its solutions. This type of culture should be initiated from induction of any student, research scholar, academician and administrator so that they can promptly decide the required action and corrective measures to avoid the cyber crime. Social media can be a better platform to initiate and understand the threat and corrective awareness. All the higher institutes should be in position to have an independent account on Face book, Twitter , YouTube and LinkedIn platform so that all kind of useful information and awareness can be shared among all and better dissemination of information can be spread to all concerned. In case of any, publicities of any events these platform play very important role. All kinds of media and video of educational related activities should be uploaded on you tube which can be seen by other too. The technical configuration and assigned roles are to properly monitored to avoid any cyber security related issues and cyber frauds. The ICT department and IT administrators are required to design the proper security guidelines for all users with prior adequate amount of training. “Students normally have an institutional e-mail address and a secure student portal, therefore regular posters and applicable CSA material should be available for them”. “In order for students to engage with CSA and establish an awareness culture, academic institutions should have the responsibility to communicate interesting and useful material”.

(Liu, Huang, and **Lucas**, 2018) Earlier examinations on records security control much of the time considers records assurance as a functional determination instead of an essential choice, and there's a deficiency of experimental investigations that utilizes documented data to contemplate network safety penetrates. We investigate how fundamental vital decisions concerning records frameworks – IT centralization, and the rethinking of records assurance – influence the likelihood of network protection penetrates with the guide of utilizing the utilization of an example of 505 U.S. better preparing foundations for a period of four year time frame. It is also find that a school which brought together of all IT choice providing and establishing the identification with less network protection breaks. Curiously, the effect

of concentrated IT administration is dependent upon the intricacy of a school's processing climate – universities with cutting edge IT foundation advantage more noteworthy from brought together administration. Furthermore, we find that revising for the self-decision predisposition, colleges that pick rethinking their records assurance have a reduction likelihood of battling from a network safety break.

(N Rjaibi and Rabai, 2017) The Mean disappointment Cost is a course of direct models that measure security dangers by thinking about the framework's partners, security prerequisites, structural segments and dangers. This quantitative network protection model adapts framework's security as far as cost which might be lost because of safety disappointment. The absence of quantitative security models in security dynamic is an approach to find qualities and uniqueness of the network protection model. This paper expects to broaden this action into a security hazard the executives model for ultra enormous frameworks and to misuse the recently introduced this model's qualities in security dynamic depending on a thorough and quantifiable examination of monetary returns. Truth be told, we plan to give a potential answer for security issues" utilizing the model to set the most noteworthy security needs and pick the reasonable countermeasures just as registering the productivity of the proposed security countermeasures through (ROI) in light of the qualities for every partner.

(Galinec, Moznik, and Guberina, 2017) Cyber security covers a wide area of multiple issues related to the sabotage of digital resoirces, and concepts closely related to information technology and communication technology (ICT) security. Cyber security is characterized by the fact that it includes the hazardous use of innovative technology to fight opponents. Cybersecurity act as a unique challenge and synonymous with ICT security that requires more and more awareness and its corrective measures to the customers and skilled security professionals to have more and more practices against the defenses and strategies that affect or depend on information technology and / or OT environments and systems In this document, our aim is to define cyber security and connect with the ways of cybersecurity. With regard to their execution, coordinated with cybersecurity strategy targetted at country level. Nine case of cyber security is presented and elaborated in the case study 87 of the Republic of Croatia and Action Plan. The maajor concern of this exercise is to identify such problems to protect and aware the society and also to viualise the importance of this issue in society.

(Burov, 2016) This paper introduced the projected conclusion and features prediction about the concern of information security with respect to a person and its related changes in HF/E in such a manner that it becomes a strong tool to analysis the target and environment of a person related activity. it also provides a mechanism to understand the nature of human in order to make he/she unprotected. Person specific psycho-physiological status defines not only a platform of dedicated efforts, but also devises a mechanism for an object to its effective control and support. It also defines that the means of a person's safety and security to be a integral segment of information habitat, networking environment, which becomes an important factor in person's activity. This paper also explores the associated cyber-security aspects and its mitigation mechanism related to all types of security threats and views regarding the cyber security challenges.

The increasing rate of such crimes in HEI's connects to various kinds of irrelevant possibilities of committing crime by using the electronic devices or a laptop for doing such kinds of unethical act in terms of theft. Most of Governments bodies have been defined this definition to understand and protect their main concern. USA fixed the definition of committing such cybercrime by using any electronic media as a unlawful activity.

Eminence higher learning Institutions having deployment of Chief Information Security Officers (CISOs) to protect their digital and research repositories to protect against any kind of cyber security challenges and also to define the cyber security policies for mitigating the challenges in case of any mishappening (Trend, 2015). In reality, such issues in the higher educational institute may happen often as cyber criminals thinks that they can easily targets such kinds of institute for their benefits (Tanya R,2015).

(Jalal and Zeb, 2015) This article mentioned the security feature of e-learning verification. This exploration reason for existing is to accomplish verification to recognize legitimate client. Web is open for all clients to access and share data. At the same time, the client programmers are additionally present, to look at a web application and framework to comprehend its plan, distinguish the possibly powerless perspectives, and utilize these shortcomings to break or adventure the application. Through confirmation measure, unlawful utilization of use can be controlled. This proposed various calculations for confirmation that is RIPEMD - 160. RIPEMD-160 catch in general secure validation. MYSQL additionally assists with giving security to information by utilizing client advantages.

(Coleman and Purcell, 2015) Information penetrates are getting more prominent not unusualplace in better tutoring. Information compromised in better tutoring penetrates extend some distance past grades; non-public and money related insights are copious at all foundations, and tricky investigations measurements are saved at numerous enormous colleges. The environmental factors of receptiveness and cooperation at schools and colleges, notwithstanding the standard get passage to of numerous movable devices make get section to less difficult for programmers and discovery of unapproved get section to troublesome. The greatest not unusual place types of insights penetrates happening in educational institute and its IT infrastructures, unplanned revelation, and movable apparatus breaks. Four colleges cases of insights penetrates examined are "Pennsylvania State University, University of Maryland, North Dakota State University System, and Butler University". Every one of the colleges talented a main measurements penetrate. The breaks had numerous similitudes, which incorporate far away get passage to and for a couple of the refinement of the assault. The entirety of the breaks have been exorbitant. School and school chiefs need to be coordinated for measurements penetrates, which remember plans to consistent for resistance to a break and respond to a break. Best practices in wellbeing and verbal trade of the polices set up preventive measures, even as digital protection, very much planned warning, and free extortion security are typical responsive measures to be needed to college and school chiefs.

(Bandara, Ioras, and Maher, 2014) The internet alludes to the unlimited boundaries of defined worlds space. Network safety sets the rules for defining safety over the usages of internet. The exploding uses and need of e-Learning frameworks has grown up exponentially by various means for conducting many examination and shows advancing development. Anyway a little consideration in this aspect has been given to the issue of safety of e-Learning frameworks both in exploration and security concern. this paper, represent a way to deal with , making assessment, observing network safety of e-Learning frameworks. Securing of these platforms and its associated frameworks helps in defining the challenges and mitigating the risks arises by using the internet by the clients of organizations. This paper also uncovers the pervasiveness of inward digital assault just as an absence of appropriate IT approaches and methodology in e-Learning frameworks.

(Coccoli, Guercio, Maresca, and Stanganelli, 2014) dissected the circumstance of training in colleges, with specific reference to the European situation. They dissect that new developments, for example, inescapable systems administration and other empowering

innovations, have been drastically changing human existence, information obtaining, and the manner in which works are performed and individuals learn. In this cultural change, colleges should keep up with their driving job. Verifiably, they set precedents basically in schooling yet presently they are called to drive the adjustment of different perspectives as well, like administration, wellbeing, and climate assurance. The accessibility of fresher and more up to date innovation thinks about how the pertinent cycles ought to be acted in the current quick changing advanced period. This prompts the selection of an assortment of shrewd arrangements in college conditions to upgrade the personal satisfaction and to work on the exhibitions of the two instructors and understudies.

(Okai, Uddin, Arshad, Alsaqour, and Shah, 2014) described dissected the circumstance of training in colleges, with specific reference to the European situation. They dissect that new developments, for example, inescapable systems administration and other empowering innovations, have been drastically changing human existence, information obtaining, and the manner in which works are performed and individuals learn. In this cultural change, colleges should keep up with their driving job. Verifiably, they set precedents basically in schooling yet presently they are called to drive the adjustment of different perspectives as well, like administration, wellbeing, and climate assurance. The accessibility of fresher and more up to date innovation thinks about how the pertinent cycles ought to be acted in the current quick changing advanced period. This prompts the selection of an assortment of shrewd arrangements in college conditions to upgrade the personal satisfaction and to work on the exhibitions of the two instructors and understudies.

(Ibrahim, 2014) examines the use of various modes of communication systems for scattered use of higher educational evaluation platform. There is a acute shortage of teaching and non teaching staff along with the required standard of technical equipments in colleges do enble the best use of the wire and wireless system. Referred paper defined majorly two main areas, the first is puzzle area of activities consisting test based software system for wireless communication and the other area is concern to security awareness and features of wireless. These types of applications were executed in a dedicated area, uses wireless local area networking in higher education.

(Alhogail and Mirza, 2014) Cyber security monitors the process which states about the process being adopted in institutions especially in educational field with the objective of guarding the IT resources and also to detect the process of employee's behavior. "The

researcher has reviewed on such security behavior, highlighted during 2003 to 2013. The primary concern was to recognize the basic structure planned monitor and control the computer security culture in HEI's. The review identified 62 papers published during era was concentrated on cyber security in HEI's research.

(Rehman, Masood and Cheema, 2013) Scholastic associations are among the most designated data frameworks on the planet. Their very decentralized set-up makes it hard to shield solid safety efforts across their organizations. Besides scholastic establishments have various divisions with different clients like personnel, staff individuals, students, and researchers and so forth who are getting to information. The chance and effect of dangers and harm to the protection, respectability and accessibility have been higher. The instructive organizations know safety of data resources,IT foundation and private research data. Personnel and understudies individual subtleties and so forth is their highest need as far as hazard and even business dependability and notoriety. It also recommends a typical structure to carry out the "Information Security Management System (ISMS) in scholarly organizations and proposes some accepted procedures to execute against the unapproved clients"

(Zeng, 2013) Cross site prearranging assaults are the most widely recognized organization assaults. Allow them the opportunity to really rehearse the assaulting exercises as programmers do and to rehearse the guard countermeasures as site directors do. In this paper they have set up an assaulting and guard lab climate for cross site prearranging instruction in higher universities. It is seen that by utilizing this lab climate understudies can more readily acknowledge what cross site prearranging weaknesses are, the reason they happen, how to accomplishment them and how to fix them. They have proposed that significantly more explores ought to be done in the space of creating assaulting and safeguard lab conditions to recuperate the results of organization security in higher professional universities.

(Neila Rjaibi, 2012) The web extends to incorporate monetary and social turn of events, network protection is currently arising "as a significant worry for analysts and professionals, managing security, classification, client verification. E-learning frameworks represent figuring frameworks and organizations of PC associated through web, as they incorporate numerous and dispersed partners, assets and information, and prime worry of secrecy, confirmation, and protection. This article characterize an exhaustive digital protection proportion of unwavering quality to measure security dangers which is the Mean Failure Cost for E-learning frameworks. The framework is proposed to permits an expert to assess the security of a framework as far as

the misfortune that every partner stands to keep up with because of safety breakdowns. The recipe to gauge the basic security necessities is additionally referenced.

(Angela Jennifa Sujana and Revathi, 2012) Distributed computing is an arising registering innovation that permits the clients to execute their own administrations utilizing on-request IT structures. The thought behind this strategy is to offer another model of arrangement which can produce versatile on-request IT foundations as per the evolving necessities. In this work specialists have proposed to utilize this on-request administration for information stockpiling particularly in HEI's. Major innovation things goes through with security issues. To tackle this issue specialists have proposed to incorporate public review capacity and information elements for Data Storage as a Service with a Trusted Third Party evaluator. In this way the proprietors of the information can put their information distantly in the cloud information stockpiling. Thus the clients can utilize that information.

(Yassir and Nayak, 2012) discusses on cyber crime in details i.e. Cyber crime which on attempt on network. Authors described network security because computers are connected on the base of network. At network hackers and other offenders will get to try access most reliable secret information or any other data with the help of malicious software or tries different types of attack on network. This paper provides how to safe used of network furthermore, a comprehension of how network security assurance can assist a firm with protecting its data and provide network management. In short it says how to use safe network (Internet) at cyber.

(Abusaimeh and Shkoukani, 2012) In research community computer network and their security are the most challenging topic in information security. Authors deep survey on web application and internet security threats. Internet security a significant subject that may affect by a internet users. In this paper they discuss difference aspect of internet and networking security and find their weaknesses along with they discuss their elements such as firewall, password, encryption, authentication and integrity. They cover attack techniques on internet and security defense technique to securing high speed internet and computer security.

3.0 Problem Statement

The role and importance of cyber security has become a vital concern in today's scenario to deal with different kinds of threats and frauds happening in and around. Inception and use of new technologies have brought the drastic change in the life style of people where the life has

become so simple in terms of performing various important and routine works. The role of societies has also changed in many ways than before. Performing of online activities which involve catering, and financial transactions of money enhancing the comfort level of individual and also making involvement of various risk factors in the forms of different frauds like loosing the personal information, loss of money or other valuable information's. The use of emails, social media and social websites may cause the different kinds of frauds in the forms of hacking the emails, hacking the website and financial transaction accounts. The higher educational institute (HEI,s) in india are catering the need of its stakeholders by imparting the various mode of educations by using the online e-learning modules and portals. E-learning portal of any Higher Educational Institute are equipped with huge number of databases and e-repositories. These databases are shared with all the required stakeholders and users to disseminate the knowledge and materials by the use of modern technology. While being online for using these resources, there are high chances to get compromise the resources by the use of malicious activities performed by the hackers .In order to avoid these issues, the role of cyber security to be exercised which will not only mitigate these challenges but also brings the awareness to all concerned (Rahim et al., 2020). The Use of Information and Communication Technology (ICT) services has come up with exemplary revolution in the life cycle of higher education management system and all its stakeholders' life. These services of ICT enhance and widen the scope of education and its existing resources which include its academic, library, teaching and Information technology services. The concepts of automation using the ICT services and latest technology have brought its all stakeholders at a single and common platform where everyone can exchange the resources and digital repositories. It encourages speedy library functions and services for access and delivery of information.

4.0 Research Objectives

The main objectives of the proposed research are as under:

- To Identify the Cyber threats and Cyber Security risks of e-Learning Portals of, and study the security trends in HE's.
- To Suggest measures to be taken to harden the e-learning portals and IT infrastructure in order to protect them from cyber attacks.
- To Prepare a reference guide / framework for securing e-learning portals and IT infrastructure with proof of concept software for implementing end point security.

4.1 Scope and Limitations of the Study

- National Capital Region (NCR) is a inter-state regional planning and development for a region with NCT-Delhi as its core. The NCR as notified covers the whole of NCT-Delhi and certain districts of Haryana, Uttar Pradesh and Rajasthan, covering an area of about 55,083 sq. kms.

Figure-. Location of universities (Sources: http://ncrpb.nic.in/ncrconstituent.html)

- The proposed study will cover Central Universities situated in Delhi and NCR. The details of universities in Delhi and NCR is mentioned in Table I. The list of the universities selected and considered for this study is mentioned below in Table II:

Table1: Details of universities in Delhi and NCR (source:internet)

	Delhi	Haryana	Uttar Pradesh	Rajasthan
Central Universities	7	1	NIL	NIL
State University	8	12	3	2
Private University	NIL	20	09	2
Deemed Universities	08	06	03	NIL

Table2: List of the Universities in Delhi (source: internet)

Sl. No	University	Year of Establishment.
1.	**Indira Gandhi National Open University** Maidan Garhi, Delhi - 110067 http://www.ignou.ac.in	1985
2.	**Jamia Millia Islamia** Jamia Nagar, Delhi - 110025 http://www.jmi.ac.in	1988
3.	**Jawaharal Nehru University** New Mehrauli Road, New Delhi – 110067 http://www.jnu.ac.in	1966
4.	**University of Delhi** University of Delhi, Delhi – 110007 http://www.du.ac.in	1922
5.	**South Asian University** Akbar Bhawan, Chanakyapuri, New Delhi http://www.southasianuniversity.org	2010
6.	**Central Sanskrit University** (Formerly Rashtriya Sanskrit Sansthana) Janakpuri, New Delhi-110058 http://www.sanskrit.nic.in	1970
7.	**Shri Lal Bahadur Shastri National Sanskrit University** (Formerly Shri Lal Bahadur Shastri Rashtriya Sanskrit Vidyapith) http://www.slbsrsv.ac.in	1962
8.	**Central University of Haryana** Mahendergarh, Haryana	2009
9.	**Indian Agricultural Research Institute** Pusa Institute New Delhi – 110012 http://www.iari.res.in	1911 Relocated in Delhi in 1936
10.	**Indian Law Institute** **Bhagwan Dass Road, New Delhi-110001** http://www.ili.ac.in	1956
11.	**Indian Institute of Foreign Trade** Qutub- Institutional Area, Delhi-110016 http://www.iift.edu	1963
12.	**NIEPA** New Delhi-110016 http://www.nuepa.org	1962
13.	**TERI School of Advanced studies** http://www.teriuniversity.ac.in	1998

14.	**Jamia Hamdard** Hamdard Nagar, New Delhi - 110062 http://www.jamiahamdard.edu	1989

- The proposed study will cover the factors associated with the usage and implementation of Information Technology in E-Learning initiative by HEI's and Cyber Security concerns.

5 Research Methodology

The methodology for the research of proposed study comprised selection of sample and population size for study, Selection of Data Collection Tools, Collection of Data, analysis of data and presentation of the results.

5.1 Selection of Sample

- The universities selected in the proposed study are Centrally funded universities situated in Delhi and NCR. Total 14 .under the category of Central and Deemed a will be selected randomly.
- The population Includes Head IT Section, Examination, Academics, Administration and Librarian.

5.2 Sample Size

- The systematic sampling method to distribute questionnaires and obtained data from users will be followed.
- The data from 28 IT Professionals which include Head –IT Section and IT professional will be gathered.
- The data from 14 Head, Academics/ Faculty, 14 Head Administration, 14 Head examination and Librarian/ Library Professional will be collected.

5.3 Sources of Data

- ***Primary Data:*** Primary Data will be collected through Questionnaires, Interviews and personal discussions.
- ***Secondary Data:*** Secondary Data will be collected through print and e resources that includes Books, Periodicals, Databases,, Internet, Websites, repositories and Handbooks/Encyclopedias and others. Review of literature has been done to understand the scope of work undertook on the cited subject area and also kind of work which had happened till now. The collected data and information would be checked with special reference to the impact in higher educational Institutes.

5.4 Data Collection Method

The research methodology is required to research, hence we are conducting a survey of Universities. Therefore survey method will be adopted in the proposed study, Two questionnaire will be prepared to get the maximum details from IT Sections and heads of Academics, Administration, Library and exams . Questionnaire is categorized in various subsections based on different aspects of required information.

- **Questionnaire:-** "Well-structured questionnaires will be prepared and also will be distributed to the heads of IT Infrastructure of the Universities". "The major objective of distributing these questionnaires to the heads of IT department will to obtain data regarding E-learning portals of Higher Education Institutes and its related fault or security issues". "The various modes of cyber security related systems enables in protection of the digital repositories from different modes of "virus attacks, macros, bugs, code problems, avoiding theft and mutilation" and to investigate technical knowledge and assess of heads of IT department involve in the maintaining the secure way of security in higher educational Institutes. "These questionnaires would be handed over to the IT heads of higher educational universities consisting the policies and plans and their relevance significance"

- **Semi- Structured Interviews:** A semi-structured interview schedule also to be used to conduct both telephone and in-person interviews with the heads of the universities' IT departments for the current study. The goal of the interviews is to supplement the quantitative data gathered through the questionnaire with more in-depth qualitative data. "This strategy provides the chance to interviewer about explaining of specific questions that a respondent is found unclear.

- **Observations of Heads of IT Departments:-** The responses received from the heads of IT department become a set process and tool for analysis of the collected data through various methods for doing research. It also provides a way to decide the expected outcomes of research area by taking care of the executed plan and Its reliability. Proper study, observation and visits would be conducted in Universities and higher educational Institutes to collect data about the e-learning portals of HEIs "such as electronic security systems, digital data security systems, computer

hardware and software security systems, physical and environmental security systems and examine its advantages and effective utilization of security measures"

5.5 Data Analysis

On the basis of the questionnaire, Observation and Interview, evaluation data will be collected and analyzed and interpreted. . The collected data will be arranged using MS-Excel.. The collected data will be analyzed with the help of SPSS Software. The Statistical techniques i.e. a.) Descriptive Statistics b.) Inferential Statistics will be employed for the analysis and interpretation. The analysis of data will be presented in the form of table diagram charts etc.

6. Expected Outcome of the Research

The expected research outcome would be to study and analyze the shortcomings of all the existing e-learning portals of higher education institutes. The major contribution of research would be to highlight the cyber security challenges and retaining issues and also to resolved them to come out with the secure e-learning portals for higher education institutes.

7. References

Abusaimeh, H., & Shkoukani, M. (2012). Survey of Web Application and Internet Security Threats. *IJCSNS International Journal of Computer Science and Network Security*, *VOL.12 No.12*, *December 2012*, *12*(12), 67–76. Retrieved from http://paper.ijcsns.org/07_book/201212/20121211.pdf

Alexei, A., & Alexei, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *Article in International Journal of Scientific & Technology Research*, *10*(3), 128–133. Retrieved from www.ijstr.org

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, *64*(2), 540–549.

Angela Jennifa Sujana, J., & Revathi, T. (2012). Ensuring privacy in Data Storage as a Service for educational institution in cloud computing. *Proceedings - 2012 International Symposium on Cloud and Services Computing, ISCOS 2012*, 96–100. https://doi.org/10.1109/ISCOS.2012.12

Bandara, I., Ioras, F., & Maher, K. (2014). CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION, (November), 728–734.

Bert Jaap Koops*,* *"*Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research*",* (Springer, 2016).

Burov, O. Y. (2016). EDUCATIONAL NETWORKING: HUMAN VIEW TO CYBER DEFENSE. *Information Technologies and Learning Tools*, *52*, 144–156.

Cheng, L. (2016). Chinese Politics in the Xi Jinping Era: Reassessing Collective Leadership. Washington, D.C.: Brookings Institution Press.

Christopher, H., & Michele, F. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Hoboken, New Jersey: Wiley

Coccoli, M., Guercio, A., Maresca, P., & Stanganelli, L. (2014). Smarter universities: A vision for the fast changing digital era. *Journal of Visual Languages and Computing*, *25*(6), 1003–1011. https://doi.org/10.1016/j.jvlc.2014.09.007

Cojocariu, A.-C., Verzea, I., & Chaib, R. (2020). Aspects of Cyber-Security in Higher Education Institutions, (May), 3–11. https://doi.org/10.1007/978-3-030-44711-3_1

Coleman, L., & Purcell, B. M. (2015). Data Breaches in Higher Education. *Journal of Business Cases and Applications*, *15*(15), 1–7. Retrieved from http://www.aabri.com/copyright.html

Filippo Parodi, “The Concept of Cybercrime and Online Threat Analysis” 2 *International Journal of Information Security and Cybercrime* 59 (2013).

Frederic, D. D. (1964). The Law Library : A living truth. In *Proceeding of 6th Biennial, Institute of Law Librarians*.

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Ibrahim, M. (2014). Utilization of Secure Wireless Networks as Environment for Learning and Teaching in Higher Education. *International Journal of Advanced Computer*, *2014*, (1). Retrieved from http://search.proquest.com/openview/60cccbfdcaa8764d243fcf2105f246be/1?pq-origsite=gscholar

Jalal, A., & Zeb, M. A. (2015). Security Enhancement for E-Learning Portal Security Enhancement for E-Learning Portal, (July).

Liu, C. W., Huang, P., & Lucas, H. C. (2018). IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. *ICIS 2017: Transforming Society with Digital Innovation*, 0–18.

M, J. M. (2014). *Information Security Systems in University Libraries of Tamil Nadu An Analytical Study*. Karunya University. Retrieved from http://hdl.handle.net/10603/117564

Maranga, M. J., & Nelson, M. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. *IJCSN-International Journal of Computer Science and Network*, *8*(4), 371–379. Retrieved from www.IJCSN.org

Okai, S., Uddin, M., Arshad, A., Alsaqour, R., & Shah, A. (2014). Cloud computing adoption model for universities to increase ICT proficiency. *SAGE Open*, *4*(3), 1–10. https://doi.org/10.1177/2158244014546461

Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology, *12*, 272–262. https://doi.org/10.29007/gprf

Rahim, N., Othman, Z., & Hamid, F. Z. (2020). Cyber security and the higher education literature: A bibliometric analysis. *International Journal of Innovation, Creativity and Change*, *12*(12), 852–870.

Rehman, H., Masood, A., & Cheema, A. R. (2013). Information security management in academic institutes of Pakistan. *Conference Proceedings - 2013 2nd National*

Conference on Information Assurance, NCIA 2013, (February 2018), 47–51. https://doi.org/10.1109/NCIA.2013.6725323

Rjaibi, N, & Rabai, L. B. A. (2017). EAI Endorsed Transactions Maximizing Security Management Performance and Decisions with the MFC Cyber Security Model : e-learning case study, *4*(1), 1–12.

Rjaibi, Neila. (2012). Cyber Security Measurement in Depth for E-learning Systems, *2*(11), 1–15.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 1–40. https://doi.org/10.3390/fi13020039

Wertkin, J. (2014). Law Librarianship 2.0. In E. Kroski (Ed.), Law Librarianship in the Digital Age (1st ed., pp. 3-12). Plymouth: Scarecrow Press.

Yassir, A., & Nayak, S. (2012). Cybercrime: A threat to Network Security. *IJCSNS International Journal of Computer Science and Network Security*, *12*(2), 84. Retrieved from http://paper.ijcsns.org/07_book/201202/20120214.pdf

Zeng, H. (2013). Research on developing an attack and defense lab environment for cross site scripting education in higher vocational colleges. *Proceedings - 2013 International Conference on Computational and Information Sciences, ICCIS 2013*, 1971–1974. https://doi.org/10.1109/ICCIS.2013.515

MANAV RACHNA
Vidyaparikshal

Dr. O.P. Bhalla Central Library
Manav Rachna International Institute of Research and Studies
(A deemed-to-be-university under section 3 of UGC Act 1956)

SIMILARITY VERIFICATION CERTIFICATE

Title: A PROACTIVE FRAMEWORK FOR DETECTING AND PREVENTING CYBER THREATS ON E-LEARNING PLATFORMS

Researcher: BHOOPENDRA SINGH Registration Number: 19/Ph.D/091

Supervisor: PROF. BRIJESH KUMAR Department: CSE - SET

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through Turnitin Software on 5/12/22 with submission ID 1971654331 and the similarity index was found to be 4 %. The complete report running into 35 Pages, 10813 Word count with File Size 5174 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date: 17/12/22

Dr. Rajesh Kumar
University Librarian
Dr. O.P. Bhalla Central Library
Manav Rachna International
Institute of Research & Studies
Faridabad

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity inde is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

Research Scholar

Research Supervisor 17/12/22

A Proactive Framework for Detecting and Preventing Cyber Threats on E-Learning Platforms

Dr. Rajesh Kumar
University Librarian
Dr. O.P. Bhalla Central Library
Maharaja Rachna International Institute of Research & Studies
17/12/22

Excluding matches less than 14 words

17/12/22

ORIGINALITY REPORT

4%	3%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Deakin University Student Paper	1%
2	eprints.eudl.eu Internet Source	<1%
3	www.iipa.org.in Internet Source	<1%
4	Submitted to IDEA Leadership & Management Institute Student Paper	<1%
5	docplayer.net Internet Source	<1%
6	mhrd.gov.in Internet Source	<1%
7	journal.iitta.gov.ua Internet Source	<1%
8	shodh.inflibnet.ac.in:8080 Internet Source	<1%
9	Sujana, J. Angela Jennifa, and T. Revathi. "Ensuring Privacy in Data Storage as a Service for Educational Institution in Cloud Computing", 2012 International Symposium on Cloud and Services Computing, 2012. Publication	<1%
10	paper.ijcsns.org Internet Source	<1%
11	www.tandfonline.com Internet Source	<1%

Exclude quotes On
Exclude bibliography On

Exclude matches < 14 words

A Proactive Framework for Detecting and Preventing Cyber Threats on E-Learning Platforms

By Bhoopendra Singh

Submission date: 05-Dec-2022 10:41AM (UTC+0530)
Submission ID: 1971654331
File name: LEARNING_PORTALS_of_HIE_s_of_NCR_FROM_EMERGING_CYBER_THREATS.doc (511.5K)
Word count: 10813
Character count: 61553